# CWE Detail – CWE-72

## Description

The product does not properly handle special paths that may identify the data or resource fork of a file on the HFS+ file system.

## Extended Description

If the product chooses actions to take based on the file name, then if an attacker provides the data or resource fork, the product may take unexpected actions. Further, if the product intends to restrict access to a file, then an attacker might still be able to bypass intended access restrictions by requesting the data or resource fork for that file.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2004-1084: Server allows remote attackers to read files and resource fork content via HTTP requests to certain special file names related to multiple data streams in HFS+.

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Read Files or Directories, Modify Files or Directories — Notes:

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** N/A

## Notes

**•** Theoretical: This and similar problems exist because the same resource can have multiple identifiers that dictate which behavior can be performed on the resource.

**•** Research Gap: Under-studied